Instituting the Privacy Officer Position

Kathy Chavis, Esq.
Privacy Officer
Department of Health and Mental Hygiene

September 2003

Definitions

- Privacy is the right of an individual to be left alone. It includes freedom from intrusion or observation into one's private affairs and the right to maintain control over certain personal information. Informational privacy is the individual's ability to control what information is available to various users and to limit re-disclosure of information.

- Confidentiality is the responsibility for limiting disclosure of private matters and includes the responsibility to use, disclose, or release such information with the knowledge and consent of the individual(s) identified; maintained through ethical behavior so that personal information is not disclosed unless called for by law, policy or the individual's express permission.

- Security is the means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss. It is the measures that are established to enable organizations and individuals to adhere to privacy expectations and to practice confidentiality in public service.

Who are Privacy Officers?

- Legal Counsel
- Risk Managers
- Compliance Managers
- Information Systems Managers
- Public Information Officer- State Gov't,§10-611
  - *Custodian.-* "Custodian" means:
  - (1) the official custodian; or
  - (2) any other authorized individual who has physical custody and control of a public record.
  - (d) *Official custodian.-* "Official custodian" means an officer or employee of the State or of a political subdivision who, whether or not the officer or employee has physical custody and control of a public record, is responsible for keeping the public record.

What does a Privacy Officer do?

- DHMH Privacy Officer – mandated by HIPAA – Healthcare model
- Someone who:
  - Anticipates and advises on potential privacy problems
  - Monitors compliance with policies, laws, regulations, and conditions of grant awards
  - Reviews proposed uses of data that have personal identifying information
  - Reviews practices related to sharing data with other agencies
  - Helps find the balance between individual rights and duties of government

What are Non-healthcare models?

- Agencies are struggling to identify the best place for the position within their organizational structures.
- Private Industry survey shows almost 50% are in Legal Counsel's Office
- Florida Legislature enacted legislation to create a state technology office whose role, in part, is to designate a state Chief Privacy Officer, responsible for the continual review of policies, rules and practices of state agencies that may affect the privacy concerns of state residents.
- The Homeland Security Department has hired a privacy officer whose job will be to ensure that activities of the new department do not erode the privacy of ordinary Americans.
  - The department will have authority to merge massive amounts of personal data from the FBI, CIA, law enforcement and other government agencies, and even private companies such as phone companies and Internet service providers to analyze for evidence that might indicate terrorist activity.

What knowledge, skills, and abilities to consider?

- The position must be granted an appropriate level of authority and oversight
- Needs to be incorporated into the agency in a manner that allows the person to effectively coordinate the development, implementation, and maintenance of an agency-wide privacy strategy
- Agencies should consider the person's ability to manage budgets, enforce compliance issues, and manage projects
- Interpreting law and regulations is only one aspect of position—must account for the integration of law, regulations and policies into business practices of the agency
- Know industry standards and legal requirements governing or directing the agency

Why have a Privacy Officer?

- Classification of data to be secured
- Coordination of activities in agencies
- Prepare for sharing data and records
- Handle Public Information Act Requests
- Emergency Communications
- Disaster Recovery
- Business Continuity

What Threats Exist to Personal Privacy

- Vast amounts of electronic information exists about individuals in public agencies
- Capacity to link to personal data
- Identity Theft

Examples of Violations

Federal and state employees have sold personal information to private investigators or other "information brokers."

- 1992 the Justice Department announced the arrest of over two dozen individuals engaged in buying and selling information from Social Security Administration (SSA) computer files
- Auditors learned that 42 employees had unrestricted access to over 130 million employment records 5 percent of the employees in one region of the IRS had browsed tax records of friends, relatives, and celebrities; Some employees used the information to create fraudulent tax refunds

What Government Collects: Public Records and Personal Records

See STATE GOVERNMENT : TITLE 10. **PART III. Access to Public Records.**

- **Generally information in government is available to everybody**
- **There are limits and what can be released generally**
  - *Adoption records* -*Welfare records*
  - *Retirement records* -*Certain police records*
  - *Personnel records* -*Student records*
  - *Maryland Transportation Authority*
  - *Motor Vehicle Administration records containing personal information*
  - *Maryland Transit Administration records*

- **(Parts of Public records that are confidential)**
  - *Medical and psychological information* -*Sociological information*
  - *Commercial information* -*Public employees*
  - *Financial information* -Notary Publics
  - *Information systems.- …* deny inspection of the part of a public record that **contains information about the security of an information system**.
  - *Professional Licensing records*

What Government Collects: Public Records

(1) "Public record" means the original or any copy of any documentary material that:

(i) is made by a unit or instrumentality of the State government or of a political subdivision or received by the unit or instrumentality in connection with the transaction of public business; and

(ii) is in any form, including:

1. a card;
2. a computerized record;
3. correspondence;
4. a drawing;
5. film or microfilm;
6. a form;
7. a map;
8. a photograph or photostat;
9. a recording; or
10. a tape.

What Government Collects: Personal Information

(1) "Personal information" means information that identifies an individual including an individual's address, driver's license number or any other identification number, medical or disability information, name, photograph or computer generated image, Social Security number, or telephone number.

(2) "Personal information" does not include an individual's driver's status, driving offenses, 5-digit zip code, or information on vehicular accidents.

What Government Collects: Personal Records

(a) *"Personal record" defined.-* In this section, "personal record" means a public record that names or, with reasonable certainty, otherwise identifies an individual by an identifying factor such as:

(1) an address; (2) a description; (3) a finger or voice print; (4) a number; or

(5) a picture.

- Each unit of State government shall post its privacy policies with regard to the collection of personal information, including the policies specified in this subsection, on its Internet website.

See Regulations at COMAR 01.01.1983.18 Privacy and State Data System Security

Disclosures of Personal Records

§ **10-626. Unlawful disclosure of personal records.**

(a) *Liability.*- A person, including an officer or employee of a governmental unit, is liable to an individual for actual damages that the court considers appropriate if the court finds by clear and convincing evidence that:

(1) (i) the person willfully and knowingly permits inspection or use of a public record in violation of this subtitle; and

(ii) the public record names or, with reasonable certainty, otherwise identifies the individual by an identifying factor such as:

1. an address;
2. a description;
3. a finger or voice print;
4. a number; or
5. a picture; or

(2) the person willfully and knowingly obtains, discloses, or uses personal information in violation of this subtitle.

Next Steps

- Assess your privacy practices against your goals and requirements as stated in law, policy, and conditions or award
- Classify data and records-Develop practical methods for protecting electronic records and document why you have the records and why they are being secured
- Identify privacy issues that will impact your security plans
- Identify whether someone in the agency is fulfilling the role
- Assess how to incorporate privacy considerations into the daily operations of your agency